Top Cybersecurity Challenges for Law Firms

Law firms large and small are making headlines for damaging data breaches. Cybercriminals often see law firms as easier targets due to a perceived weakness in their security posture. In fact, in the first two months of 2023, 10 cyberattacks were launched against six different law firms. And in 2023, the number of federal data breach class actions has skyrocketed by 154%. Law firms must step up their cybersecurity efforts to safeguard sensitive client information, protect their reputation, and avoid potentially devastating legal and financial consequences.

Top Seven Cybersecurity Challenges Facing Law Firms:

1. One-Stop-Shop for Cybercriminals

THE CHALLENGE: Not only are law firms frequently involved in high-value transactions, but they also tend to store large amounts of sensitive data in a single database. This gives cyber attackers easy access to a treasure trove of information about multiple companies—rendering law firms a highly enticing target.

THE SOLUTION: Implement a robust cybersecurity program that includes strong access controls, ongoing employee training, and regular security assessments, as well as incident response and backup and recovery plans. These plans should be complemented with regular tabletop exercises and restoration of backups.

2. De-prioritization of Cybersecurity

THE CHALLENGE: Cybersecurity is an important priority, but it can compete with other priorities, such as process transformation, digitalization, and service innovation. Allowing cybersecurity to lag in priority can lead to insufficient defenses, potentially leaving your organization more vulnerable to cyberattacks.

THE SOLUTION: Balance cybersecurity with your other top IT priorities and integrate it into your organization's strategy. Allocate funds for a CISO or other security resources to properly oversee your cybersecurity program and ensure the necessary policies, procedures, and security tools are in place. For smaller organizations, explore security outsource services.

3. Growing Compliance Complexities

THE CHALLENGE: The legal industry is subject to a variety of compliance requirements that continue to grow more complex—particularly related to data privacy and security, such as GPDR, CCPA, NY Shield, and HIPAA. Failure to comply can result in significant fines and penalties.

THE SOLUTION: Implement a holistic cybersecurity program backed by a regulatory compliance management framework, such as NIST CSF or NIST 800-53, do regular assessments against the associated controls, and put a plan in place to address any gaps.

Federal data breach class actions have skyrocketed by **154%** *(in 2023)*

dla@dlallc.com | 973-575-1565 | www.dlallc.com

Fairfield, NJ | New York, NY | Shrewsbury, NJ | Boston, MA | Chicago, IL

4. Exposure Related to Remote Work

THE CHALLENGE: As more law firms adopt a remote workplace, cybercriminals are taking advantage of the vulnerabilities associated with unsecured home networks and employee devices.

THE SOLUTION: Create, implement, and communicate cybersecurity policies and procedures to secure remote work environments, and ensure all employees understand and abide by them. Also enforce implementation of Virtual Private Networks (VPNs), multi-factor authentication, and secure Wi-Fi practices within your remote employee end user devices.

5. Security in the Cloud:

THE CHALLENGE: The shift to cloud-based platforms can result in tremendous efficiency gains, such as lower cost, improved processes, and greater productivity—but it also expands your attack surface and risk profile.

THE SOLUTION: Start by understanding the shared responsibility model of cloud computing, then protect cloud-based platforms, establish strict access controls, encrypt sensitive data, and consistently monitor for threats. Emphasizing regular compliance audits, adopting security best practices, and ensuring disaster recovery readiness are key. Rigorous vetting and management of cloud providers will further solidify the firm's cybersecurity posture in the cloud environment.

6. Third-Party Risk

THE CHALLENGE: If you work with any third-party vendors and suppliers, the security of your sensitive data is contingent on their ability to uphold rigorous cybersecurity standards.

THE SOLUTION: Regularly perform third-party assessments to ensure your vendors and suppliers are consistently following cybersecurity best practices, and monitor them to ensure they continue to meet their expected security requirements. Additionally, Identify and evaluate those vendors that are crucial to your operations and supply chain and establish contingency plans for alternative suppliers.

7. Business Email Compromise (BEC)

THE CHALLENGE: Cyber criminals are getting savvier at mimicking executives or vendors via email to trick employees into approving fraudulent transactions or revealing confidential data—and more employees are falling for it.

THE SOLUTION: Educate and train employees on how phishing campaigns work and how to avoid falling victim to such scams. Technical controls, such as email filtering and verification protocols, should also be implemented with your technology platform.

As damaging cyberattacks continue to plague the legal business community, your ability to protect your data, and swiftly respond to cyberattacks will determine whether your firm thrives in the face of a potentially catastrophic event or succumbs to its grips.

For more information about how we can help you navigate your law firm's complex cybersecurity risks, contact us here.

dla@dlallc.com | 973-575-1565 | www.dlallc.com
Fairfield, NJ | New York, NY | Shrewsbury, NJ | Boston, MA | Chicago, IL